



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/825,905	04/04/2001	Geoffrey S. Strongin	2000.050200 TT3965	3699
23720 7590 09/28/2007 WILLIAMS, MORGAN & AMERSON 10333 RICHMOND, SUITE 1100 HOUSTON, TX 77042			EXAMINER TSAI, SHENG JEN	
			ART UNIT 2186	PAPER NUMBER
			MAIL DATE 09/28/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED

SEP 28 2007

Technology Center 2100

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/825,905
Filing Date: April 04, 2001
Appellant(s): STRONGIN ET AL.

Ruben S. Bains
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on June 28, 2007 appealing from the Office action mailed on 12/19/2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Mater

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal identifies the ground of rejections and the associated claims under rejection to be reviewed on appeal.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,890,189	Nozue et al.	03-1999
4,442,484	Childs, Jr. et al.	04-1984

(9) Grounds of Rejection

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4, 7-9, 11-13, 15-17, 19-21, and 24 are rejected under 35 U.S.C. 102(b) as being anticipated by Nozue et al. (US 5,890,189).

As to claim 1, Nozue et al. disclose **a method for providing security in a computer system** [Memory Management and Protection System for Virtual Memory in Computer System (title)], **comprising:**

Controlling access to selected information [the “selected information” is “the information to be protected,” and figure 45 of Nozue shows a plurality of regions (regions 0, 1, 2, ...) each with their starting and end address and its protection key, thus the “selected information” corresponds to “the information stored in these regions”] **using attributes defined in a first table** [the table shown in figure 45 is the first table, which controls the access to each region with the attributes of protection keys, designated ownership (specific user program for each region) and the starting and ending addresses of each region];

Controlling access to the selected information using a second table [the second table is shown in figure 24A, 31, which is in the form of a TLB (column 24, lines 52-67; column 25, lines 1-67)] **that associates at least one of a read and write privilege**

Art Unit: 2186

[figure 24A, 323, shows the “r,w,x” indication of the read/write privilege] **with one or more physical address of a memory that houses the selected information** [figure 24A, 312, shows the protection associated with a plurality of physical address space, the physical page numbers; note that a page contains a plurality of physical memory addresses (figure 45 shows that a region contains 32M memory addresses defined by the START ADDRESS and the END ADDRESS; in Nozue’s invention, page and region are used interchangeably (column 14, lines 34-52)), and a reference to a physical page number applies to all the physical memory addresses within the physical page. For example, when a physical page is assigned a “w” privilege then the “w” privilege applies to all the physical memory addresses within the physical page];

receiving a request from a program to access the information [a program number uniquely assigned to each program is utilized to distinguish a plurality of programs which can make access to the memory (column 1, lines 21-26); figure 24A shows the thread numbers associated with the access requests; figures 43 and 45]; **and**

allowing access to the information in response to determining that the program has the authority to access the information based on at least one of the read and write privilege [a dedicated memory region can be secured for each program by assigning a unique program number available only to that program (column 1, lines 55-61); figure 11 shows the protection associated with a plurality of address space, the protection bits including the read permission bit (91), the write permission bit (92), and the execution permission bit (89); figure 24A, shows the “r,w,x” indication of the

read/write privilege; figure 37 shows the “r,w,x” access right associated with each program thread].

As to claim 2, Nozue et al. disclose that **controlling access to the selected information based on the privilege comprises:**
indicating in the second table that the memory housing the information is at least one of read and write disabled [the second table is shown in figure 24A, 31, which is in the form of a TLB (column 24, lines 52-67; column 25, lines 1-67); figure 24A, shows the “r,w,x” indication of the read/write allowable status; figure 34; figure 11 shows the protection associated with a plurality of address space, the protection bits including the read permission bit (91), the write permission bit (92), and the execution permission bit (89)].

As to claim 3, Nozue et al. disclose that **the second table is a bitmap based on physical addresses of the memory** [figures 11, 34, 35A, and 37].

As to claim 4, Nozue et al. disclose that **the program is an operating system** [the program may be an operating system (column 3, lines 21-26)].

As to claim 7, Nozue et al. disclose **a method for providing security** [Memory Management and Protection System for Virtual Memory in Computer System (title)], **comprising:**

writing to at least one register to define a privileged memory region [the corresponding registers comprising a current protection information register (figure 3, 17; column 13, lines 35-67), a target memory protection information register (figure 3, 18), and the starting and end address registers (figures 43 and 45). Note that the

starting and end addresses of figure 43 (figure 45 as well) fully define the range of the memory region under protection. The current protection information register of figure 3, 17 and the target memory protection information register of figure 3, 18 provide information regarding the protection of the particular instruction/data at the instant of present execution in a further finer and detailed level];

defining at least one computer instruction as a privileged instruction, wherein the privileged instruction is resident in the privileged memory region [figure 3, 14 shows the instruction access permission signal generator which defines and controls the access to a privileged memory (i.e. the instruction) region. Note that each instruction inside the privileged memory region is treated as a privileged instruction];

identifying information for protection [figure 3 shows the protection for both instruction (14) and data (15) memory];

indicating at least one physical address of a memory that houses the information as at least one of read and write disabled [figure 11 shows the protection associated with a plurality of address space, the protection bits including the read permission bit (91), the write permission bit (92), and the execution permission bit (89)]; **and**

controlling the access to the information using the privileged instruction [a dedicated memory region can be secured for each program by assigning a unique program number available only to that program (column 1, lines 55-61)].

As to claim 8, Nozue et al. disclose **writing to a second register, wherein the first and second registers define the privileged memory region** [figure 3 shows a second register, a target memory protection information register (18, column 13, lines

Art Unit: 2186

35-67); figure 43 further shows that two registers (the start and end address registers) that defines the protection region].

As to claim 9, it recites substantially the same limitations as in claim 2, and is rejected by the same reason set forth in the analysis of claim 2. Refer to "As to claim 2" presented earlier in this section for details.

As to claim 11, Nozue et al. disclose **a computer readable program storage device encoded with instructions** [figures 48, 50, and 54 show the program flow diagrams that implement the protection mechanism] **that, when executed by a computer, performs a method of providing security, comprising:**

protecting selected information using a first level of security specifying access privileges to the selected information [the first level of security is shown in the table of figure 45, which indicate which program has the privilege to access which selected information];

protecting the information using a second level of security that associates at least one of a read and write privilege with one or more addresses of a memory that houses the selected information [the second level of security is illustrated in figure 24A, 31, which is in the form of a TLB (column 24, lines 52-67; column 25, lines 1-67); figure 24A, shows the "r,w,x" indication of the read/write privilege; figure 24A shows the protection associated with a plurality of physical address space, the physical page numbers];

receiving a request from a program to access the information [a program number uniquely assigned to each program is utilized to distinguish a plurality of programs

which can make access to the memory (column 1, lines 21-26); figure 24A shows the thread numbers associated with the access requests; figures 43 and 45]; **and accessing the information in response to determining that the program has the authority to access the selected information based at least on the second security level** [figure 54, step S35, “is it access permitted by ACL, which is part of the TBL, the second table (figure 24A) based on which the second level of security is operated].

As to claim 12, Nozue et al. teach that **indicating at least one physical address of the memory includes: generating a table** [figures 11, 43 and 45] **based on the physical addresses of the memory; and indicating in the table that the memory housing the information is at least one of read and write disabled** [figure 11 shows the protection associated with a plurality of address space, the protection bits including the read permission bit (91), the write permission bit (92), and the execution permission bit (89)].

As to claim 13, Nozue et al. disclose that **the table includes an entry specifying access rights to the selected information based on one or more programs desiring to access the selected information** [figures 43 and 45 show which program ID has the right to access which memory region].

As to claim 15, it recites substantially the same limitations as in claims 1 and 15, and is rejected by the same reason set forth in the analysis of claims 1 and 15. Refer to “As to claim 1” and “As to claim 11” presented earlier in this section for details.

As to claim 16, it recites substantially the same limitations as in claim 12, and is rejected by the same reason set forth in the analysis of claim 12. Refer to "As to claim 12" presented earlier in this section for details.

As to claim 17, it recites substantially the same limitations as in claim 4, and is rejected by the same reason set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this section for details.

As to claim 19, it recites substantially the same limitations as in claim 1, and is rejected by the same reason set forth in the analysis of claim 1. Refer to "As to claim 1" presented earlier in this section for details. Further, it should be noted that although the figures do not show a processor, it is understood that a computer system inherently has at least one processor.

As to claim 20, it recites substantially the same limitations as in claim 12, and is rejected by the same reason set forth in the analysis of claim 12. Refer to "As to claim 12" presented earlier in this section for details.

As to claim 21, it recites substantially the same limitations as in claim 4, and is rejected by the same reason set forth in the analysis of claim 4. Refer to "As to claim 4" presented earlier in this section for details.

As to claim 24, it recites substantially the same limitations as in claim 1, and is rejected by the same reason set forth in the analysis of claim 1. Refer to "As to claim 1" presented earlier in this section for details.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 5-6, 10, 14, 18, 22 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nozue et al. (US 5,890,189), and in view of Childs, Jr. et al. (US 4,442,484).

With respect to claims 5, 10, 14, 18, and 22, Nozue et al. do not mention that **the information is at least one of interrupt descriptor table, global descriptor table, and local descriptor table.**

However, Childs, Jr. et al. teach in their invention "Microprocessor Memory Management and Protection mechanism" a memory management and protection mechanism in which access to protected entities is controlled. The protected entities include main memory segments, gates, task state segments, and descriptor tables [column 4, lines 17-24]. Particularly, the descriptor tables under protection are three classes of descriptor tables: interrupt descriptor table, global descriptor table, and local descriptor table [column 5, lines 20-40].

Providing protection for these descriptor tables allows full multitasking, real-time executive with task, communications, and space management facilities, as more complex microcomputer systems are usually interrupt driven [column 1, lines 20-23].

Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Appellants' invention to recognize the benefits of offering protection for descriptor tables, as demonstrated by Childs, Jr. et al., and to incorporate it into the existing memory protection mechanism disclosed by Nozue et al. to further enhance the performance of the system.

As to claim 6, Childs, Jr. et al. teach that **accessing the information in response to determining that the program has the authority to access the information includes using a stack of the computer system to verify the identity of the program** [information is pushed on the stack [column 9, lines 30-40]; Childs teaches explicitly "using a stack in the computer system to verify the identity of the program" by stating that "The caller's CPL is found in the CS selector which was pushed on the stack, and a special instruction can be used to appropriately adjust the RPL field of a selector parameter" [column 9, lines 35-39]. In other words, the caller's (i.e., the identity of the calling program) information is pushed into a stack. Further, it should be noted that claim 6 only recites the use of "a stack," and is completely silent regarding what information is stored in the stack. Thus any unique information related to a program may be pushed into a stack and be used for the purpose of identification].

As to claim 23, Childs, Jr. et al. teach that the processor disclosed in their invention is a microprocessor of the **Intel 8086** family [column 1, lines 9-19].

(10) Response to Arguments

Appellants' arguments have been fully and carefully considered with Examiner's answers set forth below.

Response to Argument A. on Claims 1-4, 19-21 and 23-24

Appellants contend that the “**physical page number**” disclosed as part of table 24A of Nozue (US 5,890,189) is not the same as the “**physical address of a memory**” as recited in claim 1, thus Nozue fails to teach this limitation. The Examiner disagrees with this argument for the following reasons:

First, the Examiner agrees that a “physical page number” does not correspond to a “single physical address of a memory;” however, a “physical page” includes “a plurality of physical addresses of a memory” and it is these physical memory addresses which are relied upon in making this rejection. When a page is referred by its “physical page number,” it applies to all the memory locations/addresses within the range of the page.

Note that the claim recites “... associated at least one of a read and write privilege with one or more physical address of a memory that houses the selected information.” Thus “a physical page” that contains “a plurality of physical addresses of a memory” certainly meets the limitation.

Also note figure 45 of Nozue shows that a region (i.e. a page; in Nozue’s invention, page and region are used interchangeably, see column 14, lines 34-52) contains 32M memory addresses defined by the START ADDRESS and the END ADDRESS.

Further, by industrial standard, a page is a fixed-size block of memory, and when used in the context of a paging memory system, a page is a block of memory whose physical address can be changed via mapping hardware [Microsoft Computer

Dictionary, 5th edition, Microsoft Press, page 386 – page; page 387 – paged address].

When a page is referred, it applies to all the memory locations/addresses within the range of the page.

Second, Nozue's invention is directed toward a memory management system where the entire memory space is organized in terms of segments and pages [figures 19-20, 33-34 and 38-40], a memory protection device is utilized in managing a logical address space divided into eight segments, where the protection is provided in units of regions representing **physical pages** in each segment, where each page is identified by a page number defined by upper 20 bits of full address [column 23, lines 29-34]. Since there is a plurality of physical pages in the memory system, a page number is assigned to each individual page for identification purpose. Again, when a page number is referred, it applies to all the memory locations/addresses within the range of the page.

Therefore, it is clear, by definition and in the context of Nozue's invention, that the "physical page number" disclosed by Nozue refers to all the memory locations/addresses specified by the range of the page, and is consistent with the element of "one or more physical addresses of a memory" recited in claim 1.

Appellants also contend that the "read/write privilege" recited in claim 1 is associated with the physical address of the memory while in Nozue's invention the "rwx" permission is associated with threads, thus Nozue fails to teach this limitation. The Examiner disagrees with this argument for the following reasons:

First, Nozue's invention is directed toward a memory management system where protection is provided in units of regions representing **physical pages** in each segment, where each page is identified by a page number defined by upper 20 bits of full address [column 23, lines 29-34]. Thus it is clear that the target of protection is the physical pages.

Second, Nozue teach that the protection of each physical page is accomplished by controlling the access to each page using the privilege of "rwx" (read, write and execution). This is clearly shown in figure 24A, where each physical page number (312) has an associated entry of "rwx" (315).

Third, it has already been established above that when a page number is referred, it applies to all the memory locations/addresses within the range of the page. Thus, the "rwx" privilege associated with each physical page is in fact associated with all memory locations/addresses within the range of the page.

Fourth, the "rwx" privilege associated with each physical page can further be modified according to individual thread accessing the page, as evident by figure 24A. Thus, different threads may have different privileges when accessing the same page. Note that the case where "rwx" privilege is associated with both the physical pages and the threads, as shown in figure 24A, is a narrower, more specific case of the more general case where the read/write privilege is associated with the memory address only. As such, Nozue's invention clearly teaches the limitation of "associate at least one of a read and write privilege with one or more physical addresses of a memory that houses

the selected information.” Refer to **MPEP 2131.02 -- Genus-Species Situations** for more information.

Appellants further contend that Examiner failed to identify the corresponding “selected information” in the first two Office Actions. The Examiner disagrees with this argument for the following reasons:

First, the Appellants are reminded that the element “selected information” is an amendment submitted by Appellants on 08/29/2005 in reply to the first Office Action mailed on 05/24/2005. It should be obvious that the Examiner was not able to address an element that did not even exist in the first Office Action.

Second, Examiner addressed the newly amended element of “selected information” in the second (and final) Office Action mailed on 10/04/2005 by referring to figure 45 of Nozue, where a plurality of regions are shown each with their starting and end address and its protection key. Figure 45 clearly identifies these regions under protection, and it should be obvious to Appellants what the corresponding “selected information” is, because Appellants repeatedly equate in their disclosure (US patent Application Publication 2002/0147916) “selected information” to “the information to be protected” (abstract; paragraphs 0007, 0010, 0022, 0048).

Third, Appellants subsequently raised the issue of what is the corresponding “selected information” in Nozue’s invention in an after-final reply dated on 12/12/2005 to the second (and final) Office Action mailed on 10/04/2005.

Fourth, Examiner addressed Appellants’ remark on the element of “selected information” in an Advisory Action mailed on 12/19/2005.

Therefore, it should be obvious that the Examiner respond in a timely manner to the issue of “selected information,” and what the corresponding “selected information” would be in Nozue’s invention.

Therefore, the Examiner’s position regarding the patentability of these claims, and those claims dependent from them, remains the same as indicated in the previous Office Action.

Response to Argument B. on Claims 11-13 and 15-17

Appellants again contend that “read and write privilege” as recited in claim 11 is associated with physical address of a memory” while Nozue’s invention associates the “rwx” privilege with threads. This issue has been fully addressed earlier (see “**Response to Argument A. on Claims 1-4, 19-21 and 23-24**”) in this Office Action.

Appellants also contend that Nozue does not teach controlling access to the “selected information” using two levels of protection. The Examiner disagrees with this argument for the following reasons:

First, it has been established earlier that the “selected information” refers to the regions under protection (see “**Response to Argument A. on Claims 1-4, 19-21 and 23-24**”).

Second, in Nozue’s invention the two levels of protection is facilitated by the two tables: the first table is shown in figure 45 and the second table is shown in figure 24A, as clearly indicated in the previous Office Action. Note that figure 45 illustrates a plurality of regions (number 0 through 6, and more), each region’s starting and end addresses, and each region’s protection key. Figure 24A further specifies the “rwx”

(read, write and execution) privilege of each physical page under protection as well as the privilege of threads when accessing each physical page under protection.

Therefore, Nozue's invention indeed provides two level of protection, via tables of figure 45 and 24A, respectively, for the "selected information," that is, regions of memory under protection.

Therefore, the Examiner's position regarding the patentability of these claims, and those claims dependent from them, remains the same as indicated in the previous Office Action.

Response to Argument C. on Claims 7-9

Appellants contend that Nozue does not teach the limitation of "writing to at least one register to define a privileged memory region in which the privileged instruction is resident." The Examiner disagrees with this argument for the following reasons:

First, regarding "writing to at least one register to define a privileged memory region," the Examiner indicated in the previous Office Action that these registers comprising a current protection information register of figure 3, 17 (page 6 of the Office Action mailed on 10/04/2005), a target memory protection information register of figure 3, 18, and the starting and end address registers of figure 43 (page 7 of the Office Action mailed on 10/04/2005). Note that the starting and end addresses of figure 43 (figure 45 as well) fully define the range of the memory region under protection. The current protection information register of figure 3, 17 and the target memory protection information register of figure 3, 18 provide information regarding the protection of the

particular instruction/data at the instant of present execution in a further finer and detailed level.

Second, Nozue's invention is directed toward providing protection to memory regions/pages, and these memory regions/pages may contain instructions or data, as illustrated in figure 3 of Nozue by the notion of "instruction access permission signal" and "data access permission signal." As the Examiner wrote in the Office Action mailed on 10/04/2005 that "each instruction inside the privileged memory region (that contains instructions) is treated as a privilege instruction" (page 6 of the Office Action mailed on 10/04/2005). Once a memory region that stores instructions is assigned certain privileges, only the users/threads given the privileges may access and execute those instructions residing in the protected region, thus all instructions of the protected region are considered as privileged instruction.

Third, as to the element of "identifying information for protection," it is note that this element is essentially the same as the "selected information" – that is, the protected memory regions/pages – as recited in claim 1, and has been addressed earlier in this Office Action (see "**Response to Argument A. on Claims 1-4, 19-21 and 23-24**"). The notion of "instruction access permission signal" and "data access permission signal" shown in figure 3 of Nozue provide further evidence that "information of protection" may include memory regions storing both instructions and data.

Therefore, the Examiner's position regarding the patentability of these claims, and those claims dependent from them, remains the same as indicated in the previous Office Action.

Response to Response to Examiner's Argument

Appellants contend that Nozue does not teach "a privileged instruction that is resident in the privileged memory region." The Examiner disagrees with this argument for the following reason.

Nozue's invention is directed toward providing protection to memory regions/pages, and these memory regions/pages may contain instructions or data, as illustrated in figure 3 of Nozue by the notion of "instruction access permission signal" and "data access permission signal." As the Examiner wrote in the Office Action mailed on 10/04/2005 that "each instruction inside the privileged memory region (that contains instructions) is treated as a privilege instruction" (page 6 of the Office Action mailed on 10/04/2005). Once a memory region that stores instructions is assigned certain privileges, only the users/threads given the privileges may access and execute those instructions residing in the protected region, thus all instructions of the protected region are considered as privileged instruction.

Response to Argument D. on Claims 5, 10, 14, 18 and 22

Appellants contend that it is not proper to combine the inventions of Nozue and Childs (4,442,484) to arrive at 35 U.S.C 103(a) rejections. The Examiner disagrees with this argument for the following reasons:

First, Childs, Jr. et al. teach in their invention "Microprocessor Memory Management and Protection mechanism" a memory management and protection mechanism in which access to protected entities is controlled. The protected entities include main memory segments, gates, task state segments, and descriptor tables

(column 4, lines 17-24). Particularly, the descriptor tables under protection are three classes of descriptor tables: interrupt descriptor table, global descriptor table, and local descriptor table (column 5, lines 20-40). Thus, this element is clearly disclosed fully by Childs.

Second, Childs explicitly provides a motivation of using interrupt descriptor table, global descriptor table, and local descriptor table in a memory management and protection system by pointing out that "Providing protection for these descriptor tables allows full multitasking, real-time executive with task, communications, and space management facilities, as more complex microcomputer systems are usually interrupt driven" (column 1, lines 20-23).

Third, both Nozue and Childs' inventions are directed toward method and apparatus of memory management and protection, thus Childs' teaching on why the use of interrupt descriptor table, global descriptor table, and local descriptor table would benefit a memory management and protection system, such as Nozue's, constitutes a direct and explicit suggestion to include these description tables to improve the performance of the system such as Nozue's.

Fourth, Childs' specifically mention that "providing protection for these descriptor tables allows full multitasking," which is exactly the type of environment that Nozue's invention is directed toward by having a plurality of threads running at the same time and may access the same protected regions.

Therefore, it would have been obvious for ones of ordinary skills in the art at the time of Appellants' invention to recognize the benefits of offering protection for

descriptor tables, as demonstrated by Childs, Jr. et al., and to incorporate it into the existing memory protection mechanism disclosed by Nozue et al. to further enhance the performance of the system.

Therefore, the Examiner's position regarding the patentability of these claims remains the same as indicated in the previous Office Action.

Response to Argument E. on Claim 6

Appellants contend that claim 6 should be allowable because it recites "using a stack in the computer system to verify the identity of the program" while the references teach "using a stack to adjust a privilege level field." The Examiner disagrees with this argument for the following reasons:

First, Nozue explicitly teaches "verifying the identity of the program" in figure 45, where it shows that a plurality of user programs (column PROGRAM NAME) are associated with a plurality of memory regions (column REGION NO.) that are defined by their respective starting address (column START ADDRESS), end address (column END ADDRESS) and protection key (column PROTECTION KEY). Thus the identity of the user program allowed to accessing each protected region is well defined and must be verified in order to enforce the protection.

Second, although Nozue explicitly teaches "verifying the identity of the program," Nozue does not mention "using a stack" as an implementation tool.

However, Childs teaches explicitly "using a stack in the computer system to verify the identity of the program" by stating that "The caller's CPL is found in the CS selector which was pushed on the stack, and a special instruction can be used to appropriately


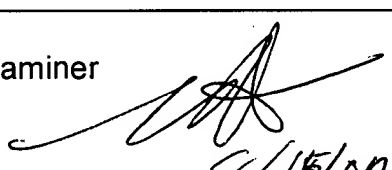
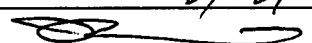
adjust the RPL field of a selector parameter" (column 9, lines 35-39). In other words, the caller's (i.e., the identity of the calling program) information is pushed into a stack.

It should also be noted that claim 6 only recites the use of "a stack," and is completely silent regarding what information is stored in the stack. Thus any unique information related to a program may be pushed into a stack and be used for the purpose of identification.

Therefore, the Examiner's position regarding the patentability of this claim remains the same as indicated in the previous Office Action.

(11) Related Proceedings Appendix

None.

Sheng-Jen Tsai Examiner Art Unit 2186	 8/15/2007
Matthew Kim Supervisory Patent Examiner Art Unit 2186	 8/15/07
Lynne H Browne Appeal Practice Specialist, TQAS Technology Center 2100	

August 15, 2007